NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Appendix B Glossary

Term	Definition
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.
Acceptance	The act of an authorized representative of the Government by which the Government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether a facility or system meets the

	specified technical and performance standards.
Access	Access is the ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection).
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accountability	The security goal that generates the requirement for actions of NASA management to be traced uniquely to a specific NASA resource. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Account Authorization Official	The NASA Center official with authority and responsibility for all aspects of policy, business operations, and operational life cycle for NAMS. The Center AAO is the primary technical representative and provides guidance and oversight of the daily activities and personnel supporting NAMS. The Center AAO represents all Center NAMS activities and operations to Agency-level committees with oversight responsibility for NAMS implementations across NASA.
Accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency

	operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed upon set of security controls.
Accreditation Package	The evidence provided to a NASA authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.
Acquisition	All stages of the process of acquiring property or services, beginning with the process for determining the need for the property or services and ending with contract completion and closeout.
Active Content	Active content refers to electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user. Active content technologies allow mobile code associated with a document to execute as the document is rendered.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls.

Administratively Controlled Information (ACI)	Certain official information and material which is not national security information (and therefore cannot be classified), nonetheless, should be protected against disclosure. Such information and material, which may be exempt from disclosure by statute or is determined by a designated NASA official to be especially sensitive, shall be afforded physical protection sufficient to safeguard it from unauthorized disclosure. Within NASA, such information has previously been designated "FOR OFFICIAL USE ONLY." This designation has been changed for clarity and to more accurately describe the status of information to be protected. (See NPG 1620.1, Section 4.4.7 for specifics.)
Application	The use of information resources (information and information technology) to satisfy a specific set of user requirements (reference OMB A-130). Also, a set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as "system software."
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.

Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Auditing	Auditing is the review and analysis of management, operational, and technical controls. The auditor can obtain valuable information about activity on a computer system from the audit trail. Audit trails improve the auditability of the computer system.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
Authorization	Authorization is the permission to use a computer resource. Permission is granted, directly or indirectly, by the application or information system owner.
Authorizing Official	A NASA official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency

	operations (including mission, functions, image, or reputation), Agency assets, or individuals.
Availability	As defined in FISMA, the term 'availability' means ensuring timely and reliable access to and use of information [44 USC 3542 (b)(1)(C)].
Background Investigation	The means or procedures used to determine the suitability of an individual to have privileged or limited privilege access and to hold a "Public Trust" position. Conducted by the Center Chief of Security.
Baseline Set of Security Controls	The minimum security controls recommended for an information system based on the system's security categorization established in accordance with FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems (prepublication final), December 2003.
Certification	Certification is a formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer, rather than one involved in building the system. Certification is more often cost-effective for complex or high-risk systems. Less formal security testing can be used for lower-risk systems. Certification can be performed at many stages of the system design and implementation process and can take place in a laboratory, operating environment, or both.

Certification Agent	The individual, group, or organization responsible for conducting security certification.
Chief Information Officer (CIO)	Agency official responsible for: (1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, and regulations, and the priorities established by the head of the agency; (2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (3) promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	Individual responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.
Clinger-Cohen Act of 1996	A statute that substantially revised the way that IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.

Common Security Control	Security control that can be applied to one or more NASA information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control may have been applied.
Compromise	Disclosure of information to unauthorized persons or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Computer Security	The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information/data, and telecommunications).
Computer Virus	A computer virus is similar to a Trojan horse insofar as it is a program that hides within a program or data file and performs some unwanted function when activated. The main difference is that a virus can replicate by attaching a copy of itself to other programs or files and may trigger an additional "payload" when specific conditions are met.

Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.
Contracting Officer	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
Contracting Officer's Technical Representative	An individual to whom the CO delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues.
Cost-Benefit Analysis	When considering security, cost-benefit analysis is done through risk assessment, which examines the assets, threats, and vulnerabilities of the system in order to

	determine the most appropriate, cost-effective safeguards (that comply with applicable laws, policy, standards, and the functional needs of the system). Appropriate safeguards are normally those whose anticipated benefits outweigh their costs. Benefits and costs include monetary and non-monetary issues such as prevented losses, maintaining an organization's reputation, decreased user friendliness, or increased system administration.
Counterintelligence	The term "counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities [50 USC 401a].
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module [FIPS PUB 140-2].
Deliverable	A product or service that is prepared for and delivered to the Government under the terms of a contract.

Denial of Service	The prevention of authorized access to resources or the delaying of time-critical operations.
Development/Acqui-sition	During this phase the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.
Disposal of Assets	Releasing the accountability (excessing, turned in for repair, or transferring to another organization) of IT equipment and ensuring the elimination of any controlled information and software stored on this equipment.
Encryption	The translation of data into a form that is unintelligible without a deciphering mechanism.
Event	Any observable occurrence in a network or system.
Exhibit 300	The Exhibit 300 business case is a high-level summary of the investment's current justification and management plans, including a project plan, benefit-cost analysis, alternatives analysis, acquisition plan, risk management plan, human resources management plan, enterprise architecture, and IT Security plan. In the case of proposed new IT investments, this information is used by the operating unit, the department's Capital Investment Technology Review Board (CITRB), and OMB to determine if the investment should be recommended for funding. For

	ongoing investments, the Exhibit 300 is used to review the investment's current status and, subsequently, to assess how well the investment accomplished its goals. In addition, the Exhibit 300 is required when requesting a delegation of procurement authority from the CIO through the CITRB or the Acquisition Review Board to proceed with a large contract. It is expected that the Exhibit 300 information is supported by more detailed plans for acquisition, risk management, alternatives, benefit-cost analysis, project scheduling, security and earned value management.
Exhibit 53	Section 53 describes IT portfolio data (major projects) reporting requirements and focuses on how such investments should be linked to the President's Management Agenda (PMA), E-government. "Major IT system or project means a system that requires special management attention because of its importance to an agency mission. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should be evaluated against ["major" IT system or project] criteria... Additionally, if the project or initiative directly supports the President's Management Agenda items, then the project meets the criteria of "high executive visibility." Projects that are E-Government in nature or use e-business technologies must be identified as major projects regardless of the costs."

External Customers or Groups	Those who are not affiliated in any way with the entity with which they are conducting business. In this document, these customers may include Federal, State, or local Governments; international partners; other NASA organizations; or organizations in the private sector.
Facility	Designated locations in which a logical group of one or more IT resources are located.
Federal Information Processing Standards (FIPS)	Issued by the NIST after approval by the Secretary of Commerce regarding management and operations of IT resources. (Also called FIPS PUBS.)
FIPS PUB	An acronym for Federal Information Processing Standards Publication. FIPS publications (PUB) are issued by NIST after approval by the Secretary of Commerce. Some FIPS PUBs are mandatory for use in federal acquisitions.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

General Support System	General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Hostile Probes	The act of using one or more systems to scan targeted systems or networks with intent to conduct or to gather information for unauthorized activities. They are often targeted against networks (LAN's) rather than single stand-alone systems. They may return information that may provide information on system vulnerabilities.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.
Intrusion Detection System	A software application that can be implemented on host operating systems or as network devices to monitor for signs of intruder activity and attacks.
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Implementation	After initial system testing, the system is installed or fielded.
Inappropriate Usage	A person who violates acceptable computing use policies.
Incident	An adverse event or situation associated with a system which poses a threat to the integrity, availability, or confidentiality of data or systems and that results in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of Government property or information.
Individual Accountability	Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Information	Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, such as computerized databases, paper microfilm, tapes, disk, memory chips, RAM, ROM, microfiche, communication lines, and display terminals.
Information Assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection,

	detection, and reaction capabilities [CNSS 4009].
Information Owner	The individual (organizational line manager) responsible for the confidentiality, integrity, and availability of a specific set of data. This individual is responsible for making judgments and decisions on behalf of the organization with regard to the data's information category level, criticality, use, protection, and sharing. Typically, this individual is a member of the organization directly supported by the data. This individual often maintains the data and ensures its accuracy. All data have a data owner.
Information Resource Management	The planning, budgeting, organizing, directing, training, and control of information and related resources, such as personnel, equipment, funds, and technology.
Information Security Policy	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System	The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems are also referred to as IT systems within this document.
Information System Security Official	The principal staff advisor to the information system owner on all matters involving the ITS of the information system. This responsibility may also

	include physical security, personnel security, incident handling, and security training and education.
Information Technology	The term "information technology," with respect to an executive agency, means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.
Information Technology Resources	Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or

	reception of data. This includes telecommunication systems, network systems, and human resources. (Also called Automated Information Resources.)
Information Technology (IT) System	See information system.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity - Accountability	The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Accountability. A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
Integrity - Authenticity	Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Authenticity. A third party must be able to verify that the content of a message has not been changed in transit.
Integrity - Non-repudiation	The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to: Non-repudiation. The origin or the receipt of a specific message must be verifiable by a third party.

Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Intelligence	The term "intelligence" means (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term "intelligence" includes foreign intelligence and counterintelligence [Joint Pub 1-02] [50 USC Ch 15].
International Partner	Foreign entities with which business and/or research is conducted. International partners may include individuals, small firms, large corporations, and/or foreign governments.
Internet Protocol (IP)	A standard designed for use in interconnected systems of packet-switched computer communication networks. The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fix-length addresses.
Intrusion Detection	Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.

Intrusion Detection System (IDS)	A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both.
IP address	An IP address is a unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
Information Owner	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System Owner	An agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. Responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the security requirements.
Information System Security Official	The information system security official (ISSO) is the principal staff advisor to the information system owner on all matters involving the IT security of the information system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. For smaller systems, a system administrator may perform the ISSO role as well as the

	system administrator role.
Keystroke Monitoring	Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.
Local Area Network (LAN)	A Local Area Network (LAN) is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a Wide Area Network (WAN).
Logon	The identification and authentication sequence that authorizes a user's access to a computer. Conversely, "logoff" is the sequence that terminates user access to the system.
Major Application	Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Malicious Code	Malicious code refers to programs that are written intentionally to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses, computer viruses, and worms.
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Mandatory Requirements	Those contractual conditions and technical specifications that are established by the Government as being essential to meeting required needs.
Master System Security Plan	A Master, or "umbrella," system security plan (SSP) is a document which provides an overall picture of the security of the systems under an Agency Associate Administrator's responsibility (or equivalent per NITR-4) and is a key component of the certification and accreditation process. Master SSPs are to be supported by subordinate system security plans for individual systems. The difference between a master and a subordinate SSP is that the master primarily provides direction for the security of the subordinate systems that are included under it. Certification testing of security controls is to be done at the subordinate SSP level.

Media	Any and all materials in which data and/or information may be stored and may include floppy disks, CD-ROMS, hard drives, software manuals, and papers.
Memorandum of Understanding/ Agreement (MOU/A)	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
Mission Essential Infrastructure (MEI)	Critical infrastructures, physical, Cyber-based systems, or a combination, whose diminished capabilities would significantly impact the Federal Government's ability to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; and the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. (Reference Presidential Decision Directive (PDD) 63, May 22, 1998.)
Mobile Code	Mobile code refers to programs (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics. The term also applies to situations involving a large homogeneous collection of platforms (e.g., Microsoft

	Windows).
Monitoring	An ongoing activity that checks on the system, its users, or the environment.
Multiple Component Incident	A single incident that encompasses two or more incidents.
National Security Information	Information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
Network	An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking...) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, commerce services provider, or relying party).
Network Address Translation	An Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box, located where the LAN meets the Internet, makes all necessary IP address translations. NAT serves three main purposes: (1) provides a type of firewall by hiding internal IP addresses;

	(2) enables a company to use more internal IP addresses (both are used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations); and (3) allows a company to combine multiple ISDN connections into a single Internet connection.
Network Administrator	A person who manages a local area network (LAN) within an organization. Responsibilities include network security, installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.
Networks	Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.
OMB A-130, Appendix III	Establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information; and

	links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.
Operation/Mainte-nance	After initial system testing, the system is installed or fielded. Many security activities take place during the operational phase of a system's life. In general, these fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Organization Computer Security Official	The designated Government person who is assigned the task of managing and maintaining the security of IT resources within a component.
Password	A string of characters used to authenticate an identity or to verify access authorization. [FIPS PUB 140-1]
Patch	A patch (sometimes called a "fix") is a "repair job" for a piece of programming. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker's Web site. The patch is not necessarily the best solution for the problem, and the product developers often find a better solution to provide when they package the product for its next release. A patch is

	usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and track the installation of patches.
Patch Management	The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.
Penetration Test	A planned attempt by authorized officials to circumvent security controls in order to identify security weaknesses that need to be corrected.
Personal Use	Activities conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using IT resources to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using IT resources to support a personal private business also includes employees using IT resources to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of IT resources to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization (examples).

Plan of Action and Milestones	The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. POA&Ms are used to close security performance gaps, assist the Inspector General (IG) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities. The POA&M presents the opportunity for an agency to highlight its progress and demonstrate improvements in the quality and security of its information security program. It is also designed to serve as a management tool specific to agency processes and as a point of comparison for OMB in its assessment of the overall maturity of the Federal Government's IT security status. Though the POA&M is considered a comprehensive plan, OMB operates under the assumption that additional and more detailed project management plans exist for each corrective action item identified in the POA&M, and that additional sources (e.g., IG audit reports and risk assessments) are readily available to provide original documentation of each weakness. Thus, each POA&M element should be clearly traceable back to its original source(s).
Potential Impact	Low: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or

	individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Privacy Act of 1974 (Pub. Law 93-579)	A law enacted by Congress to protect against an invasion of privacy through the misuse of records by Federal agencies which allows a citizen to learn how records are collected, maintained, used, and disseminated by the Federal Government. It also permits an individual to gain access to most personal information maintained by Federal agencies and to seek amendment of any incorrect or incomplete information.
Privileged Access	That which is granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.
Procedural Controls	Security measures that IT system managers impose through personnel actions rather than by electronic means. Also called administrative controls. Examples of procedural controls include using sign-in logs, documenting configuration changes, and filling out checklists.

Remote Logon	Accessing one system by way of another without having to log on to the destination host. For example, accessing System B by logging on to System A and linking directly from System A to System B without logging on a second time.
Request for Information (RFI)	An announcement requesting information from industry in regard to a planned acquisition and, in some cases, requesting corporate capability information.
Request for Proposal (RFP)	A formal solicitation document used in negotiated acquisitions normally exceeding $100,000 to communicate government requirements and to solicit proposals.
Request for Quotation (RFQ)	A less formal solicitation document used in negotiated acquisitions valued at $100,000 or less to communicate government requirements and to solicit quotations.
Residual Risk	The portion of risk remaining after the application of appropriate security controls in the information system.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Analysis	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that

	mitigate this impact. Part of risk management and synonymous with risk assessment.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes: risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal approval to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Risk Mitigation	Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints.
Risk Reduction	The lessening of security exposure to an acceptable level. This requires the identification, analysis, selection, approval, and implementation of cost-effective IT security protective measures. Sometimes called "safeguard

	implementation."
Rules of Behavior	Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Safeguards	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Scanning	Sending packets or requests to another system to gain information to be used in a subsequent attack.
Security	Security is a system property. Security is much more that a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms, which span the system both logically and physically.

Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Certification	A comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Security Impact Analysis	The analysis conducted by an agency official often during the continuous monitoring phase of the security certification and accreditation process to determine the extent to which changes to the information system have affected the security posture of the system.

Security Objectives	The five security objectives are integrity, availability, confidentiality, accountability, and assurance.
Security Plans	The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.
Security Policy	The statement of required protection of the information objects.
Security Requirements	Requirements levied on an information system derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
SAISO	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Sensitive Information	Sensitive Information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could

	adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.
Sensitive But Unclassified	Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.
Sensitivity	Sensitivity in an information technology environment consists of the system, data, and applications which must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability which is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.
Serious Adverse Impact	An event causing temporary harm resulting in a negative effect on: mission or project schedules or cost; the confidentiality, integrity, and availability of "special management attention" or high or moderate impact systems; or the image and reputation of NASA. The consequence would be recoverable; but at a cost in tangible assets or resources (one million dollars or less), in customer or public confidence, and place NASA at a financial or technological disadvantage.

Significant Change	A modification, deletion, or addition to a system which may result in reducing the effectiveness of protective controls or in making additional protective controls necessary. Examples of significant changes include, but are not limited to, relocation to other facilities, major modification of the existing facilities, introduction of new equipment, addition or deletion of external interfaces, changes to system network connectivity, installation of new operating system software, patches to applications, new releases of software, installation of new application software, introduction of more sensitive data, or a substantial change to the system's risk posture that might affect others on the same network.
Social Engineering	The act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network.
Statement of Work	A statement of the technical specification in the RFP that describes the material, product, service, or system required by the Government.
Subordinate System Security Plan	A subordinate system security plan (SSP) is a document, which provides an overall picture of the security of the systems under a program, project, or

	system-owner's responsibility, and is a key component of the certification and accreditation process. Subordinate SSPs support the master SSP. The master SSP primarily provides direction for the security of the subordinate systems that are included under it. Certification testing of security controls are to be accomplished at the subordinate SSP level.
System	A system, as defined by this guideline, is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must: (1) be under the same direct management control; (2) have the same function or mission objective; (3) have essentially the same operating characteristics and security needs; and (4) reside in the same general operating environment.
System Administrator	A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System Interconnection	The direct connection of two or more IT systems for sharing data and other information resources.
System Operational Status	System Operational Status is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
TCP/IP	Transmission Control Protocol/Internet Protocol is the protocol suite used by the Internet. A protocol suite is the set of message types, their formats, and the rules that control how messages are processed by computers on the network.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Telecommunications	The term "telecommunications" means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Uniform Resource Locator URL	A Uniform Resource Locator is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, the two URLs below point to two different files at the domain nist.gov. The first specifies an executable file that should be fetched using the FTP protocol; the second specifies a Web page that should be fetched using the HTTP (Web) protocol: ftp://www.nist.gov/stuff.exe; http://www.nist.gov/index.html.
Update	An update (sometimes called a "patch") is a "repair" for a piece of software (application or operating system). During a piece of software's life, problems (called bugs) will almost invariably be found. A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software vendor's Web site. The patch is not necessarily the best solution for the problem, and the

	product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module). In larger operating systems, a special program is provided to manage and keep track of the installation of patches.
User Account	Authority granted to an individual to access a system or software application. Typically granted by system administrators with the approval of the system's line manager. To access an account, a user needs to be authenticated, usually by providing a password.
User Authentication	A process by which a system receives validation of a user's identity.
Verification	The process used by an independent agent to confirm or establish by testing, evaluation, examination, investigation or competent evidence, the effectiveness of the security controls in an information system.
Virtual Private Network (VPN)	A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them.
Virus	See Computer Virus.

Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Wireless Local Area Network (WLAN)	A type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov